REMARKS

Claims 1-3, 5-7, 10, 11, 13, 14, 16-22, 25-27, 29, 31, 34-50, 58, and 59 have been amended.

Claims 1-66 are pending

Rejections

Claims 1-66 stand rejected under 35 U.S.C.§102(b) as being anticipated by U.S. Patent No. 4,835,682, issued to Kurachi et al (hereinafter referred to as *Kurachi et al*). Applicants respectfully disagree with the rejections for at least the following reasons.

Kurachi et al. disclose techniques for preventing unauthorized copying of software programs stored on floppy drives. To do this, *Kurachi et al.* take advantage of a floppy disk controller/drive that supports two different frequency modulation modes, namely a standard frequency modulation (FM) mode and a non-standard frequency modulation mode (MFM). *Kurachi et al.* also utilize a machine ID associated with the host computer that is attempting to load a program that is stored on a floppy disk using the MFM mode. In order to read the floppy disk, the host computer is required and configured to convert the MFM written program and rewrite it to the floppy disk using the FM mode. During the rewrite to the floppy disk, the program is modified based on the machine ID such that when the floppy disk is read in the future only the host computer will be allowed to run the modified program stored on the floppy disk. *Kurachi et al.* teach that the modified program is de-modified and the resulting original program is then allowed to run. If the rewritten floppy disk is subsequently inserted into another

computer having a different machine ID, the program cannot be de-modified and therefore cannot be run.

Independent Claim 1, is drawn to a method that includes having at least one computer receive unique key data from at least one other computer. The at least one computer then converts the initial digital good into a modified digital good using the unique key data to selectively individualize the initial digital good for use with the computer, such that the modified digital good has a substantially unique operative configuration that properly functions with the computer. The method also includes causing the at least one computer to run the modified digital good. *Kurachi et al.* fail to disclose or reasonably suggest a modified digital good, which while customized for use on a given computer, can be run. Instead, *Kurachi et al.* teach that their modified program is de-modified and the resulting original program is then allowed to run. Here, in accordance with certain aspects of the present invention, the modified program is unique in its operative configuration for the given computer and runs.

Claim 2, which depends from Claim 1, further specifies that the conversion act further includes manipulating at least one flow control operation within the initial digital good. *Kurachi et al.* fail to disclose or reasonably suggest the notion of manipulating the flow control of the program. Indeed, *Kurachi et al.* teach that their modified program needs to be de-modified to reproduce the resulting original program.

Claim 3, which depends from Claim 1, further specifies that at least one other computer generates the unique key data based on at least one unique identifier data associated with the computer. *Kurachi et al.* fail to disclose or

reasonably suggest having another computer generate any key data. Indeed, *Kurachi et al.* teach that the computer uses its own internal machine ID.

Claim 4, which depends from Claim 3, further specifies that the method allows for selective limitations on the operation of the modified digital good to computers that are properly associated with at least the unique identifier data. *Kurachi et al.* fail to disclose or reasonably suggest having other properly associated computers run the program. Indeed, *Kurachi et al.* teach that only the computer can run their de-modified program.

Claim 5, which depends from Claim 3, further specifies that the method includes causing the at least one computer to provide the unique identifier data associated with the at least one computer to the at least one other computer, and causing the at least one other computer to cryptographically generate the unique key data based on the unique identifier data provided by the at least one computer and at least one secret key. *Kurachi et al.* fail to disclose or reasonably suggest having the computer provide unique identifier data to other computers or having other computers cryptographically generate unique key data based as recited in Claim 5. Indeed, *Kurachi et al.* teach that the computer can use its machine ID to verify if the de-modified program (i.e., their original program) can be run.

Claim 6, which depends from Claim 3, further specifies that the at least one other computer generates at least a first key and a second key, and the first key and the second key are different, but cryptographically related to the secret key, and wherein the received unique key data includes the first key. *Kurachi et al.* fail to disclose or reasonably suggest having another computer generate multiple related cryptography keys based in part on provided unique identifier data. Indeed, *Kurachi et al.* are silent when it comes to cryptography and key generation,

especially when their computer simply uses its machine ID to modify the program and later de-modify the program so it can be run in its original configuration.

Claim 7, which depends from Claim 1, recites that the method further includes dividing the initial digital good into at least a first portion and a second portion using the at least one other computer, providing the first portion to the at least one computer via a first computer readable medium, and subsequently providing the second portion to the at least one computer via a second computer readable medium. *Kurachi et al.* fail to disclose or reasonably suggest having another computer divide their original program and provide them portions using at least two mediums. Instead, *Kurachi et al.* focus only on the delivery of their non-standard frequency modulation mode (MFM) written program on a floppy drive.

Claim 8, which depends from Claim 7, further recites that the first computer readable medium includes a different type of computer readable medium than the second computer readable medium. Again, *Kurachi et al.* focus only on the delivery of their MFM written program on a single two-sided floppy drive.

Claim 9, which depends from Claim 8, further recites the first computer readable medium includes a fixed computer readable medium and the second computer readable medium includes a network communication. As before, Again, *Kurachi et al.* focus only on the delivery of their MFM written program on a single two-sided floppy drive.

Claim 10, which depends from Claim 7, further recites that the method includes having the at least one other computer convert the second portion into a modified second portion using the unique key data to selectively manipulate at least one flow control operation within the second portion, such that the modified second portion is operatively different in configuration to the second portion, and

providing the modified second portion to the at least one computer via the second computer readable medium. *Kurachi et al.* fail to teach these additional features.

Kurachi et al. also fail to teach the additional features recited in the following claims: **Claim 11**, which depends from Claim 10, further recites that the at least one other computer is used to convert the second portion into the modified second portion. **Claim 12**, which depends from Claim 10, further recites that the unique key data includes at least a first key and a second key, and converting the second portion into a modified second portion further includes using the second key to selectively manipulate at least one flow control operation within the second portion. **Claim 13**, which depends from Claim 10, further recites that the unique key data includes at least a first key and a second key, and that providing the second portion to the at least one computer further includes providing the first key to the at least one computer. **Claim 14**, which depends from Claim 13, further recites that the at least one computer converts the first portion into a modified first portion using the first key to selectively manipulate at least one flow control operation within the first portion, such that the modified first portion is operatively different in configuration, and that the at least one computer operatively combines the modified first portion and the modified second portion to produce the modified digital good. **Claim 15**, which depends from Claim 13, further recites selectively limiting operation of the modified digital good to computers that are properly associated with at least the first key.

Claim 16, which depends from Claim 3, recites that the method further includes having the at least one computer to provide the unique identifier data associated with the at least one computer to the at least one other computer, and accessing computer identification data within the at least one computer and

including the computer identification data within the unique identifier data associated with the at least one computer. **Claim 17**, which depends from Claim 16, further specifies receiving user identification data at the at least one computer and including the user identification data within the unique identifier data associated with the at least one computer. While *Kurachi et al.* teach that machine IDs can be used within open computer, they fail to teach that other data may be used and/or that user identification data can be received and included in the unique identifier data that is provided to the other computer.

Consequently, claims 1-17 are patentable over *Kurachi et al.*

The remaining claims will be summarized as they share at least some of the same novel differences as one or more of the claims presented above. Here, **Independent Claim 18** recites a computer that receives an initial digital good and unique key data from at least one other computer, and converts the initial digital good into a modified digital good using the unique key data to selectively individualize the initial digital good for use with the at least one computer, such that the modified digital good has a substantially unique operative configuration that properly functions with the computer. *Kurachi et al.* fail to teach this claimed invention. **Claims 19-26**, which depend at least in part on Claim 18, recite further limitations similar to Claims 2-17. Again, *Kurachi et al.* fail to teach these claimed inventions. Hence, Claims 18-26 are patentable over *Kurachi et al.*

Independent Claim 27 is directed towards a computer-readable medium comprising computer-executable instructions for receiving unique identifier data associated with at least one computer, generating unique key data based on at least the unique identifier data, converting at least a portion of an initial digital good using the unique key data to selectively individualize the portion of the initial

digital good, such that a modified portion of the digital good is produced that is operatively different in configuration, and providing at least the modified portion of the digital good and at least a portion of the unique key data to the at least one computer. For at least the reasons described above, Claim 27 is patentably distinct from *Kurachi et al.* Depending from Claim 27 and adding still further novel limitations are **Claims 28-33**, each of which is patentable too over *Kurachi et al.* for at least the reasons presented above.

Independent Claim 34 is directed towards an apparatus for use in a host computer. The apparatus includes an individualizer that is configured to receive unique key data and at least a portion of an initial digital good from at least one source computer, and produce at least a portion of a modified digital good using the unique key data to selectively individualize the initial digital good for use with the host computer, and such that the modified digital good is operatively different in configuration than the initial digital good. For at least the reasons described above, Claim 34 is patentably distinct from *Kurachi et al.* Depending from Claim 34 and adding still further novel limitations are **Claims 35-42**, each of which is patentable too over *Kurachi et al.* for at least the reasons presented above.

Independent Claim 43 recites an apparatus for use in a source computer. Here, the apparatus includes a key generator that is configured to receive a unique identifier data from a destination computer and generate unique key data based on the received unique identifier data associated with the destination computer. The apparatus also includes an individualizer configured to receive the unique key data and at least a portion of an initial digital good and output at least a portion of a modified digital good using the unique key data to selectively individualize the initial digital good, such that the modified digital good is operatively different in

configuration than the initial digital good. For at least the reasons described above, Claim 43 is patentably distinct from *Kurachi et al.* Indeed, *Kurachi et al.* fail to have there source computer and destination computers communicate at all. Depending from Claim 43 and adding still further novel limitations are **Claims 44-49**, each of which is patentable too over *Kurachi et al.* for at least the reasons presented above.

Independent Claim 50 recites a system that includes an identifier configured to output unique identifier data associated with a computer, a key generator coupled to receive the unique identifier data and generate at least one unique key data based on the received unique identifier data, and at least one individualizer configured to receive the unique key data and at least a portion of an initial digital good and output at least a portion of a modified digital good using the unique key data to selectively individualize the initial digital good, such that the modified digital good is operatively different in configuration than the initial digital good. For at least the reasons described above, Claim 50 is patentably distinct from *Kurachi et al.* Depending from Claim 50 and adding still further novel limitations are **Claims 50-66**, each of which is patentable too over *Kurachi et al.* for at least the reasons presented above.

Thus, as illustrated in the examples above, Claims 1-66 are each patentable over *Kurachi et al.* Consequently, it is respectfully requested that the rejections be reconsidered and withdrawn.

Conclusion:

The pending claims are clearly patentable over the cited art.

Respectfully Submitted,

Dated: 9/30/02

By: _____

Thomas A. Jolly
Reg. No. 39,241
(509) 324-9256